**IN THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA, Plaintiff, v. ANTON PERAIRE-BUENO, and JAMES PERAIRE-BUENO, Defendants.	Case No.: 1:24-cr-00293-JGLC **[FILED PARTIALLY UNDER SEAL]**

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF JOINT MOTION TO COMPEL PRODUCTION OF *BRADY* MATERIAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULE

OTHER AUTHORITIES

The government's obligation to search for and produce exculpatory information is well-established by *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny. *See, e.g.*, *Giglio v. United States*, 405 U.S. 150 (1972); *United States v. Agurs*, 427 U.S. 97, 106-07 (1976); *United States v. Bagley*, 473 U.S. 667, 682-83 (1985); Fed. R. Crim. P. 5(f). Defendants Anton and James Peraire-Bueno made specific requests (among others) to the government for the following exculpatory material:

> (1) Material tending to show that the alleged Victim Traders were engaged in trading strategies known as "sandwich attacks" on the Ethereum network;
>
> (2) Material tending to show that sandwich attacks are a form of market manipulation; and
>
> (3) Information regarding the anonymity of the alleged Victim Traders, including refusals to identify themselves, known steps they have taken to hide their identities, and requests for anonymity and the reasons for seeking anonymity.

The government has refused to search for and produce any of this material pursuant to *Brady*. The government does *not* claim this information does not exist. Rather, the government argues this information is not favorable to the defense or, to the extent it is discoverable, it is only through *Giglio* and 18 U.S.C. § 3500.[1] For the reasons discussed in detail below, that contention incorrect; the requested material is exculpatory because it undermines particular Indictment allegations and supports potential defense theories regarding the Peraire-Buenos' specific intent. The Peraire-Buenos move for an order compelling the government to search for and produce any material responsive to these requests pursuant to its *Brady* obligations.

[1] Declaration of Katherine Trefz ("Trefz Decl.") ¶ 3.

I. BACKGROUND[2]

The Indictment alleges that the Peraire-Buenos committed wire fraud and money laundering in connection with a novel trading strategy executed on the Ethereum Network. Indict. ¶ 1. The Ethereum Network is a decentralized cryptocurrency platform that is not run by a central actor. *Id.* ¶ 7.

The first two categories of the requested *Brady* material bear directly on several Indictment allegations relating to the norms that supposedly exist on the Ethereum Network and the alleged roles and expectations of its users. Without a citation to any particular authority or set of established rules or regulations, the Indictment makes dozens of allegations about the way trading on the Ethereum Network functions, what "typical[]" trading strategies look like, how the alleged Victim Traders and Peraire-Buenos fit into that environment, and how "rules and protocols" are implemented. *Id.* ¶¶ 7-15, 22, 24-26.

The third category of Brady material relates to the significance of anonymity on the Ethereum Network. The Indictment alleges that the Peraire-Buenos' intent to defraud is shown in part because they "took numerous steps to conceal their identities and lay the groundwork to conceal the stolen proceeds, including by setting up shell companies and using multiple private cryptocurrency addresses and foreign cryptocurrency exchanges." *Id.* ¶ 2.

On July 16, 2024, the Peraire-Buenos made numerous requests for discovery, including specific *Brady* requests. *See* Trefz Decl., Ex. 1. They reiterated certain of those requests that are the subject of this motion by letter on September 26, 2024. *Id.*, Ex. 2. On October 11, 2024, the

[2] A longer description of the Indictment's allegations is contained in Defendants' Joint Motions to Dismiss at 3-9, also filed today.

government informed the Peraire-Buenos that it did not view those requests as seeking exculpatory material pursuant to *Brady* and would not be searching for it. *Id.*, Ex. 4.

II. LEGAL STANDARD

As *Brady* and its progeny explain, the Fifth Amendment requires the government to disclose all evidence in its possession that is favorable to the accused and material to guilt or punishment. *Brady v. Maryland*, 373 U.S. 83, 87 (1963). This obligation applies to all documents and information in the government's possession regardless of whether individual prosecutors have personally reviewed the information, *see Giglio v. United States*, 405 U.S. 150, 154 (1972); *United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998), and even if it is not captured in "tangible form" like a document or email, *United States v. Rodriguez*, 496 F.3d 221, 226 (2d Cir. 2007). "A *Brady* violation occurs when the government fails to disclose evidence materially favorable to the accused." *Youngblood v. West Virginia*, 547 U.S. 867, 869 (2006) (per curiam); *see United States v. Coppa*, 267 F.3d 132, 140 (2d Cir. 2001).

Evidence is "favorable to an accused" where it tends to exculpate the defendant (such as by undermining Indictment theories or supporting potential defense theories), impeaches the credibility of a government witness (including hearsay declarants), or tends to mitigate punishment. *United States v. Bagley*, 473 U.S. 676-77 (1985); *Giglio*, 405 U.S. at 154-55; *Brady*, 373 U.S. at 88-90; *United States v. Jackson*, 345 F.3d 59, 70-71 (2d Cir. 2003). Material need not be entirely exculpatory to be subject to disclosure, *United States v. Mahaffy*, 693 F.3d 113, 130 (2d Cir. 2012); *United States v. Rivas*, 377 F.3d 195, 199-200 (2d Cir. 2004), and it need not be admissible if it could lead to the discovery of admissible evidence, *Mahaffy*, 693 F.3d at 131.

III. THE COURT SHOULD COMPEL THE GOVERNMENT TO SEARCH FOR AND PROVIDE THE REQUESTED MATERIAL.

As discussed below, each specific *Brady* request seeks exculpatory material that reasonably could affect the outcome of the trial. The Peraire-Buenos understand that the government refuses to search for and provide this material based on the claim that it is not substantively favorable to the Peraire-Buenos. The government is wrong. The Court should compel the government to search for and promptly provide any material responsive to these requests. *See* Fed. R. Crim. P. 5(f) Order, ECF 38 at 1.

A. Requests 1-2: Material Tending to Show the Alleged Victim Traders Were Engaged in Market-Manipulating Sandwich Attacks Is Exculpatory.

The Indictment alleges that the Peraire-Buenos committed fraud by acting in contravention of the purported "rules and protocols" of a decentralized blockchain that no central actor runs. Thus, the expectations of the various participants in the Ethereum Network are central to the Indictment's allegations. The Indictment contains sweeping allegations regarding trading on Ethereum generally and the roles of various users of the MEV-Boost system specifically. Indict. ¶¶ 7-14. These allegations about the typical roles and expectations appear to underpin the Indictment's theory—to the extent it has one—for what was allegedly fraudulent about the alleged transactions at issue. *See id.* ¶¶ 17, 24-27, 35, 37.

Evidence that undermines the Indictment's allegations about the norms and expectations of the users in the trading environment that the Peraire-Buenos allegedly violated is exculpatory. To that end, the Peraire-Buenos have made two related requests that are the subject of this motion[3]: (1) for material tending to show that the alleged Victim Traders were engaged in trading strategies

[3] The requests at issue in this motion do not cover the full landscape of potentially exculpatory information about the trading environment. *See* Trefz Decl., Ex. 1.

known as "sandwich attacks" and (2) for material tending to show that sandwich attacks are a form of market manipulation. As discussed below, the material sought by both requests would be exculpatory because it would undermine the Indictment's theory of typical cryptocurrency trading and its allegations about how individuals—including the alleged Victim Traders—interact with each other, would support the picture of the trading environment as an adversarial and trustless place, and would support a good-faith defense regarding what is permitted on the Ethereum Network.

1. The Indictment's Allegations Regarding "Typical[]" "MEV Bot" "Arbitrage" Trades.

The Indictment alleges that the Victim Traders were engaged in transactions "typical[]" of "automated" "MEV Bots" and that this "typical[]" activity was regular cryptocurrency arbitrage. Indict. ¶¶ 13, 22, 24. The Indictment makes these allegations in several steps. First, the Indictment alleges that "searchers" are cryptocurrency traders that look for arbitrage opportunities through automated bots ("MEV Bots"). *Id.* ¶ 13. It then goes on to allege what it claims is a "typical[]" trade proposed by an arbitrage MEV Bot in this environment. *Id.* It alleges that a "typical[]" proposed trade is a "bundle" consisting of particular transactions "in a precise order": (1) a "'frontrun' transaction, in which the searcher purchases some amount of cryptocurrency whose value the searcher expects to increase"; (2) a "pending transaction in the mempool" (*i.e.*, a transaction proposed by another trader that has not yet been added to a block) "that the MEV Bot identified would increase the price of that cryptocurrency"; and (3) "the searcher's sell transaction, in which the searcher sells the cryptocurrency at a higher price than what the searcher initially paid in order to extract a trading profit." *Id.*

2. Evidence Undermining These Allegations Is Exculpatory.

Evidence tending to show that the Indictment's characterization of typical trading and arbitrage is incorrect would be favorable to the defense. In fact, what the Indictment casts as "typical[]" behavior is *not* typical arbitrage; instead, it is widely recognized as *malicious* behavior (or at least controversial behavior) known as a "sandwich attack."

a. The Victim Traders were sandwich attackers.

A "sandwich attack" is trading behavior that preys on retail users of the Ethereum Network by manipulating prices within individual liquidity pools[4] where users seek to trade a certain amount of Currency Token X for a certain amount of Currency Token Y. Such attacks exploit unsophisticated users on the Ethereum blockchain using the transparency afforded by the blockchain: as the Indictment alleges, "[w]hen a user conducts a transaction on the Ethereum blockchain, such as a buy or sell trade, this transaction is not immediately added to the blockchain. Instead, the pending transaction waits alongside other pending transactions in the 'memory pool' or 'mempool,' which is publicly visible." Indict. ¶ 9. Because of the delay, pending transactions usually have some price flexibility built in to the proposed trade—the user says they will pay the current price and up to a particular percentage more if the market moves; that extra amount is known as "slippage." Sandwichers take advantage of this transparency and slippage by searching for proposed transactions whose price they can drive up in the liquidity pool through the "frontrun" transaction. Those proposed transactions are the sandwicher's potential targets; the "blockchain

[4] Liquidity pools enable users on a decentralized exchange to engage in peer-to-peer trading without the need for a broker or market maker. The pools are smart contracts that contain two or more cryptocurrencies (or tokens representing that cryptocurrency) so that a user can easily exchange one for the other. *See Liquidity Pool*, Coinbase, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/liquidity-pool (last accessed Nov. 30, 2024); Cryptopedia Staff, *What Are Liquidity Pools?*, Cryptopedia (Nov. 16, 2023), https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity#.

attacker sandwiches [the transaction] between two transactions to make a profit." *What is a sandwich attack?*, Uniswap, https://support.uniswap.org/hc/en-us/articles/19387081481741-What-is-a-sandwich-attack (last accessed Nov. 30, 2024) (hereinafter, "Uniswap Website").

Uniswap, the cryptocurrency exchange on which the alleged transactions were executed, summarizes the steps for making this "sandwich" as follows:

> 1. A user [*i.e.*, the victim of the sandwich attacker] submits a swap, and it is pending confirmation.
>
> 2. A blockchain attacker [*i.e.*, the alleged "victims" here] sees the pending transaction, and knows the price for the token swapped will increase. So, they submit a swap. This is called *front-running*.
>
> 3. The blockchain attackers [*sic*] swap is completed at a low price.
>
> 4. The user's transaction is completed at a high price, which means they receive less tokens than expected.
>
> 5. The blockchain attacker swaps the tokens again at a higher price. This is called *back-running*.

Id.; *see* Indict. ¶ 13 (describing alleged victims' desired order of transactions here). By bundling proposed trades in this way, "[t]he blockchain attacker profits from the increase in price from the previous transactions," which in the end, "results in a gain for the attacker, and a loss for the user." Uniswap Website. In other words, the sandwich causes the sandwich victim to pay more for Currency Token Y than they otherwise would have without the frontrun. Then, taking advantage of that increased price, the sandwicher's back-run transaction effectively brings the price of Currency Token Y down to approximately where it would have been without the frontrun.[5]

[5] *See also, e.g.*, *What are sandwich attacks in crypto?*, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-are-sandwich-attacks-in-crypto (last accessed Dec. 3, 2024); *What Are Sandwich Attacks in Crypto? A Beginner's Guide*, Unchained, https://unchainedcrypto.com/sandwich-attacks-crypto/ (last accessed Nov. 30, 2024).

The government knows that the three alleged victims in this case were all sandwich attackers. IRS-CI Special Agent Marco Dias swore as much in support of an application for a search warrant to Google, LLC for vast troves of stored electronic information. *See* Trefz Decl., Ex. 8 ¶¶ 17(b) (referring to alleged victims' trades as "sandwich trades"), 17(h) (using a schematic that referred to the alleged victims' trades as "sandwich [transactions]" or "sandwich attack bundle[s]"); *see also id.* ¶ 16(c)(i)-(iii) (describing steps in alleged victim trades). Indeed, the alleged Victim Traders in this case [redacted] *See, e.g.*, Trefz Decl., Ex. 7.

b. Sandwich attacks are widely considered to be malicious market manipulation, not typical arbitrage.

Sandwich attacks are *not* typical arbitrage. Typical arbitrage tends to enhance the efficiency of trading markets by identifying and correcting differences among *different* markets.

> [Arbitrage] refers to a specialized form of trading which is said to be based upon disparity in quoted prices of the same or equivalent commodities, securities, or bills of exchange. In its most common form, it involves purchase of a commodity against a present sale of the identical commodity for future delivery—time arbitrage; or a purchase in one market, say New York, against a sale in another, such as London—space arbitrage.

Falco v. Donner Found., Inc., 208 F.2d 600, 603 (2d Cir. 1953) (citing among other sources Loss, Securities Regulation, at 589 & n.426 (1951) and 12 CFR § 220.4d(2)); *see also Mirman v. Berk & Michaels, P.C.*, 1994 WL 410881, at *1 n.1 (S.D.N.Y. Aug. 3, 1994) ("Arbitrage is the profiting from differences in price when the same security, currency, or commodity is traded on two or more markets.") (citing Downes and Goodman, Dictionary of Finance and Investment Terms (3d ed. 1991)). Generally speaking, arbitrage trading is considered to be consistent with market efficiency; in other words, by eliminating or reducing price disparities across markets, arbitrageurs promote the efficiency of markets. *See In re PolyMedica Corp. Sec. Litig.*, 432 F.3d 1, 8-10 (1st Cir. 2005) (discussing academic literature on arbitrage trading and market efficiency). In contrast, sandwich attacks do *not* occur across "different markets," but within a single liquidity pool, with their effects limited to and reversed by the bundle they propose.

Rather than typical arbitrage, sandwich attacks are considered to be a form of market manipulation by many in the crypto community. Coinbase describes "sandwich trading" as a "form of market manipulation" that "exploits price discrepancies to profit at the expense of other traders," "undermines trust in the market," and "can deter legitimate participants." *What are sandwich attacks in crypto?*, Coinbase ("Sandwich attacks are a form of *market manipulation* on decentralized exchanges.") (emphasis added)[6]; *see also, e.g.*, *What Are Sandwich Attacks in Crypto? A Beginner's Guide*, Unchained ("A sandwich attack in the DeFi markets is a type of market manipulation that occurs on decentralized exchanges (DEXs), where a malicious actor spots a large pending transaction and places two transactions around it: one before and one after the targeted transaction.");[7] *Sandwich Trading*, Binance Academy ("Sandwich trading, also known as sandwich attacks or sandwiching, is a trading strategy or *manipulation technique* in the cryptocurrency markets") (emphasis added).[8] And some cryptocurrency platforms punish actors for engaging in sandwiching or otherwise disallow it. *See, e.g.*, Jordan Leech, *Solana Foundation removes certain operators from delegation program over malicious sandwich attacks*, The Block (June 20, 2024) (reporting that a prominent cryptocurrency foundation, Solana, recently removed

[6] *Available at* https://www.coinbase.com/learn/crypto-glossary/what-are-sandwich-attacks-in-crypto (last accessed Nov. 30, 2024).

[7] *Available at* https://unchainedcrypto.com/sandwich-attacks-crypto/ (last accessed Nov. 30, 2024).

[8] *Available at* https://academy.binance.com/en/glossary/sandwich-trading (last accessed Nov. 30, 2024).

from its platform a group of "validator operators" who perpetrated "sandwich attacks on Solana users").[9]

This view makes sense, even when the government's own framing of the alleged victims' goals is considered. In his affidavit in support of a search warrant, Agent Dias noted that the "only valu[e]" of a sandwicher's proposed bundle is the "sequential order," *i.e.*, that both the front-run and the back-run execute, Trefz Decl., Ex. 8 ¶ 16(c)(iii); no doubt that is because the basic purpose is to obtain trading profits from the victim, not to invest in cryptocurrency, *see What are sandwich attacks in crypto?*, Coinbase.[10] The government has argued in other cases that is a hallmark of market manipulation. *See, e.g.*, Transcript, *United States v. Eisenberg*, No. 23-cr-10 (AS) (S.D.N.Y.), ECF 170 at 1341 (Gov't summation) (arguing that "[p]umping," meaning manipulating a cryptocurrency market to increase the price of a token, is "not trading" and "not an investment" but rather "criminal"); *id.* (contrasting "taking the market into his own hands" with making "a great investment"); *id.* (describing "creating a price" as "cheating" that manipulates the market).

c. Evidence that the Victim Traders were sandwich attackers and that sandwich attacks are market manipulation is exculpatory.

Evidence tending to show that the Victim Traders were sandwich attackers and that such activity is considered market manipulation would be favorable to the defense for a number of reasons. First, as noted above, evidence that undermines or provides a counter-narrative to the Indictment's picture of the trading environment and its purported norms and expectations is exculpatory. Evidence indicating the alleged victims' trading behavior was not "typical," as the

[9] *Available at* https://www.theblock.co/post/299244/solana-foundation-removes-certain-operators-from-delegation-program-over-malicious-sandwich-attacks.

[10] *Available at* https://www.coinbase.com/learn/crypto-glossary/what-are-sandwich-attacks-in-crypto (last accessed Nov. 30, 2024).

Indictment alleges, but is manipulative, undermines that picture. Similarly, evidence tending to show that the alleged victims were engaged in adversarial trading—*i.e.*, using their own accounts to victimize other users on the network for their own profit-maximizing purposes—would tend to support a view of the alleged "Exploit," Indict. ¶ 1, as an adversarial-but-permissible defense against a sandwich attack occurring in a decentralized, trustless environment. This counter-narrative would undermine the government's proof of falsity and intent. *Cf. United States v. Braunstein*, 281 F.3d 982, 995-96 (9th Cir. 2002) (evidence that the alleged victim knew of and tacitly condoned distributors' "gray market" practices so undermined government's wire-fraud theory as to render prosecution "frivolous").

Second, the acknowledgement and use of the terminology itself is favorable to the defense because it tends to support a view that the jargon used in the industry does not necessarily align with the common usage. For example, description of a particular event as an "attack" or an "exploit" or "malicious" may sound inherently illegitimate in common parlance, but that does not mean that it is illegal or even discouraged on the Ethereum Network. Thus, to the extent that the government seeks to show that the transactions at issue in the Indictment were fraudulent because *others* called the alleged "Exploit" by the Peraire-Buenos "malicious," an "exploit," or an "attack," the requested evidence would undermine the probative value of the use of those phrases. Indeed, the Indictment uses phrases such as "exploit" and "malicious validator" that appear designed to carry some weight (emotional, if not legal), and the common industry usage of such terms for all sorts of activities on the Ethereum Network would undermine the impact of such terms.

Third, evidence that sandwich attacks like those made by the Victim Traders are a form of market manipulation—or were actively being debated as such within the industry—also undermines the government's ability to prove intent at a higher level. The government must prove that the Peraire-Buenos had specific intent to defraud. If behavior widely considered to be manipulative—or even illegal[11]—is not only permitted within the Ethereum Network but is now being *vindicated* by the United States government, that tends to make more likely an explanation that the Peraire-Buenos did not believe that their own alleged actions were fraudulent. Evidence of a defendant's good faith should be broadly construed and not normally limited. *See United States v. Litvak*, 808 F.3d 160, 190 (2d Cir. 2015) (district court abused its discretion in finding irrelevant evidence that other traders were engaged in allegedly illegal behavior because such evidence was relevant to good faith); *United States v. Collorafi*, 876 F.2d 303, 305 (2d Cir. 1989); *United States v. Brandt*, 196 F.2d 653, 657 (2d Cir. 1952).

Notably, these requests are not made in support of an "everyone was doing it, and therefore, it is not *illegal*" defense. In its letter explaining why it would not search for these materials, the government cited *United States v. Connolly*, 2019 WL 2125044, at *13 (S.D.N.Y. May 2, 2019), for the proposition that "everybody is doing it" is not a defense. Trefz. Decl., Ex. 4 at 1 (alteration omitted). But that is not the argument here. The Peraire-Buenos do not contend that their alleged trading strategy was not illegal because the alleged Victim Traders were engaged in the same behavior. After all, the Peraire-Buenos were not sandwich attackers. Rather, their argument is (1) the fact that the alleged victims were engaged in adversarial, even malicious behavior is relevant to the alleged expectations and norms in the decentralized trading environment identified in the

[11] Unlike general arbitrage trading, market manipulation is usually considered illegal. For example, 7 U.S.C. § 13 makes it a crime for "[a]ny person to manipulate or attempt to manipulate the price of any commodity in interstate commerce," and virtual currencies have been determined to be commodities under the Commodity Exchange Act, *see, e.g.*, *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228-29 (E.D.N.Y. 2018). The Southern District of New York charged Avi Eisenberg with market manipulation by making a series of large purchases in order to artificially increase the price of one currency relative to another. *See* Indict., *United States v. Eisenberg*, No. 1:23-cr-10 (AS) (S.D.N.Y.), ECF 4, ¶ 3.

Indictment, and (2) the known actions of others are relevant to a defense good-faith argument. *Connolly* was not to the contrary. It assessed whether the government had ultimately *proven* intent beyond a reasonable doubt pursuant to Federal Rule of Criminal Procedure 29. It did not find evidence of others' crimes irrelevant; in fact, it cited *Litvak*'s holding that such evidence *is* relevant, if potentially less probative than other evidence. 2019 WL 2125044, at *13.[12]

B. Request 3: Material Tending to Show the Alleged Victims' Efforts and Desire to Remain Anonymous Is Exculpatory.

The Indictment alleges that the Peraire-Buenos took steps to conceal their identities and that this desire for some degree of anonymity is indicative of bad intent. *See* Indict. ¶¶ 2-3. But pseudonymity is a well-recognized value in cryptocurrency markets: while there is substantial transparency as to the *transactions* that take place on the blockchain, the users typically interact through pseudonyms and it is often not easy to find the true identities of the various users.[13] To that end, the Peraire-Buenos requested the government provide information regarding the

[12] The government offers no other reason for its refusal to produce these favorable materials. Its mistaken belief about how the Peraire-Buenos would use this evidence demonstrates the problems inherent in the government making pre-trial determinations about whether specifically requested evidence is helpful or material. Numerous courts have cautioned prosecutors to err on the side of disclosure rather than second-guess a defendant's judgment. *See, e.g.*, *Agurs*, 427 U.S. at 108 ("[T]he prudent prosecutor will resolve doubtful questions in favor of disclosure."); *United States v. Van Brandy*, 726 F.2d 548, 552 (9th Cir. 1984) ("[W]here doubt exists as to the usefulness of evidence, [the government] should resolve such doubts in favor of full disclosure."). And where, as here, the defendant furnishes specific rather than general *Brady* requests, the materiality analysis should take that fact into account. *See Agurs*, 427 U.S. at 106. ("[I]f a substantial basis for claiming materiality exists, it is reasonable to require the prosecutor to respond either by furnishing the information or by submitting the problem to the trial judge. When the prosecutor receives a specific and relevant request, the failure to make any response is seldom, if ever, excusable.").

[13] *See, e.g.*, *Van Loon v. Dep't of Treasury*, --- F.4th ---, 2024 WL 4891474, *2 (5th Cir. Nov. 26, 2024) (pseudonymity); *id.* at *5 (identifying legitimate reasons for using mixers to provide additional anonymity); Cryptopedia Staff, *Anonymity vs. Pseudonymity In Crypto*, Cryptopedia (May 17, 2021), https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences.

anonymity of the alleged Victim Traders, including their refusals to identify themselves (even to law enforcement), known steps they have taken to hide their identities, requests for anonymity, and the reasons for such actions.

The exculpatory nature of such material is obvious when considered alongside the allegations in the Indictment. Material showing that, like the Peraire-Buenos allegedly did, other users in the market—including in the transactions at issue—made efforts to conceal their identities would tend to support a defense argument that a desire for anonymity is not a sign of criminal intent in this trading environment, and similarly is not inconsistent with good faith. Additionally, the alleged Victim Traders' reasons for desiring anonymity may support other defenses. For example, if the alleged Victim Traders are associated with sanctioned entities, criminal enterprises, or potentially illegal activity and sought to remain anonymous as a result, this information may support an innocent explanation for the Peraire-Buenos' alleged refusal "to return the stolen cryptocurrency," Indict. ¶ 1, or their own alleged efforts to remain anonymous from malicious actors.

There is reason to believe such information exists in the government's possession. As discussed in the concurrently-filed Motion for a Bill of Particulars regarding the identity of the Victim Traders, the identity of two of the three alleged Victim Traders is unknown to the Peraire-Buenos, and it is not clear the government has even identified them. (Neither the Indictment nor the discovery suggests the government has.) To the contrary, documents contained in the Rule 16 productions indicate that the alleged Victim Traders [redacted]. *See* Trefz Decl., Exs. 6, 7.

C. The Government Should Not Be Permitted to Wait for Its *Giglio* and 18 U.S.C. § 3500 Disclosures.

It is not sufficient for responsive material to be included in the *Giglio* or 18 U.S.C. § 3500 disclosures that the government will make by September 16, 2025. As described above, such material is not simply impeaching but is exculpatory and the government has an independent obligation to provide it under *Brady*. And it is unclear how § 3500 is relevant; limitations on discovery in the Jencks Act do not lessen the government's "independent obligation to timely produce exculpatory material under Brady." *United States v. Rittweger*, 524 F.3d 171, 181 n.4 (2d Cir. 2008). The Court's August 19 Order requires the government to produce exculpatory material "promptly after its existence becomes known to the Government so that the defense may make effective use of the information in the preparation of its case." Fed. R. Crim. P. 5(f) Order, ECF 38 at 1. Here, this material may be used to develop and identify admissible evidence, including but not limited to expert testimony, disclosures for which are due well in advance of September 16, 2025.

IV. CONCLUSION

For all of the above reasons, the Court should compel the government to search for and produce

(1) Material tending to show that the alleged Victim Traders were engaged in trading strategies known as "sandwich attacks" on the Ethereum network;

(2) Material tending to show that sandwich attacks are a form of market manipulation; and

(3) Information regarding the anonymity of the alleged Victim Traders, including refusals to identify themselves, known steps they have taken to hide their identities, and requests for anonymity and the reasons for seeking anonymity.

Date: December 6, 2024

Respectfully submitted,

By: *<u>/s/ Katherine Trefz</u>*

Katherine Trefz (*pro hac vice*)
Daniel Shanahan (*pro hac vice*)
Patrick J. Looby (*pro hac vice* pending)
Williams & Connolly LLP
680 Maine Avenue SW
Washington, DC 20024
Tel: (202) 434-5000
ktrefz@wc.com
dshanahan@wc.com
plooby@wc.com

Jonathan P. Bach
Shapiro Arato Bach
1140 Avenue of the Americas
17th Floor
New York, NY 10036
Tel: 212-257-4897
jbach@shapiroarato.com

Counsel for Defendant
James Peraire-Bueno

By: *<u>/s/ Daniel M. Marx</u>*

Daniel N. Marx
William W. Fick (*pro hac vice*)
Fick & Marx LLP
24 Federal Street, 4th Floor
Boston, MA 02110
Tel: 857-321-8360
dmarx@fickmarx.com
wfick@fickmarx.com

Counsel for Defendant
Anton Peraire-Bueno

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2024, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this matter who are on the CM/ECF system.

/s/ Katherine Trefz
Katherine Trefz